UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,430	12/04/2003	Mark L. Buer	2875.0240001	6875

26111 7590 10/17/2008

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
POWERS, WILLIAM S	
ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
10/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/727,430	BUER ET AL.	
	Examiner	Art Unit	
	WILLIAM S. POWERS	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,7-10,12,15-18,20-24,27,33,40,51-53,56 and 58-68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,7-10,12,15-18,20-24,27,33,40,51-53,56 and 58-68* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/22/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 9/4/2008 have been fully considered but they are not persuasive.

2. As to Applicant's argument that, "Yang does not teach or suggest 'process[ing] at least a portion of the received internal [outbound] packet if the security processor address data matches address information associated with the security processor'" (Remarks, p. 15, lines 10-12), the Examiner respectfully disagrees. The Applicant has replaced the limitation "security processor identifier" with "security processor address data" to the independent claims. The Examiner sees no distinction between the replaced limitation and the newly amended limitation. The Applicant is directed to col. 6, lines 32-38 of Yang where the SA_ID is an example of SA index or indices which is used to lookup SA fields in order to perform processing on the packet (Yang, col. 6, lines 52-65). The Examiner views index or indices as examples of addresses that are used to locate Security Association policies through lookups in order to apply required IP processing. It is inherent, if not obvious, that if the SA_ID does not match a lookup index, processing is not performed. For at least the reasons above, the rejection of the amended claims is maintained.

Response to Amendment

3. The Examiner has stated the below column and line numbers as examples. All columns and line numbers in the reference and the figures are relevant material and

Applicant should be taken the entire reference into consideration upon the reply to this Office Action.

4. Claims 1, 8, 10, 16, 18, 21, 23, 27, 33, 40, 51-53 and 59 have been amended.

5. Claims 4-6, 11, 13, 14, 19, 25, 26, 28-32, 41-50, 54, 55 and 57 have been cancelled.

6. Claims 34-39 have been withdrawn from consideration.

7. Claims 1-3, 7-10, 12, 15-18, 20-24, 27, 33, 40, 51-53, 56 and 58-68 are pending.

Response to Amendment

Information Disclosure Statement

8. The Information Disclosure Statement submitted 9/22/2008 has been considered by the Examiner.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

10. Claims 1-3, 7, 33, 40, 56 and 60-62 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent No. 7,003,118 to Yang et al. (hereinafter Yang).

As to claims 1 and 33, Yang teaches:

a. Receiving, by a security processor, an internal outbound packet from an Ethernet controller (the apparatus of Yang is used in an Ethernet environment that processes TCP/IP packets using IPSec protocols) (Yang, col. 2, lines 8-26 and line 60-col. 3, line 4), wherein the internal outbound packet includes a flow identifier for the internal outbound packet and a security processor address data (packet has an SA_ID (flow identifier) , data indicating the type of security processing required and the SA_ID is an index (address) used to lookup SA fields for IP processing) (Yang, col. 5, line 58-col. 6, line 48).

b. Processing at least a portion of the received internal outbound packet if the security processor address data matches address information associated

with the security processor (SA_ID is used as an index lookup to apply IP processing to the packet. It is inherent, if not obvious, that the indices have to match in order for the IP processing to be executed on the packet.) (Yang, col. 6, lines 1-48), wherein the processing includes:

i. Using the flow identifier as a direct address handle to retrieve a security association for the received internal outbound packet (SA_ID is the security association identification associated with the packet and is used as an index to obtain the appropriate keys and IP processing for the packet) (Yang, col. 6, lines 1-65).

ii. Performing a cryptographic operation on a portion of the received internal outbound packet using at least a portion of the retrieved security association (required processing is executed on the outbound packet to include cryptographic operations) (Yang, col. 6, line 66-col. 7, line 8).

iii. Assembling an outbound network packet including a header and the cryptographically processed portion of the received internal outbound packet (IPSEC Tx Data State Machine assembles outbound packet after processing) (Yang, col. 7, lines 28-49).

iv. Transmitting from the security processor, the outbound network packet (IPSEC Tx Data State Machine transmits outbound packet after processing) (Yang, col. 7, lines 28-49 and fig. 4).

As to claim 2, Yang teaches wherein performing the cryptographic operation comprises performing one or more IPSec operations (accelerator of Yang is used in an IPSec environment) (Yang, Title and Abstract).

As to claim 3, Yang teaches wherein the IPSec operations comprise adding or removing protocol elements (adding IP elements) (Yang, claim 19).

As to claim 7, Yang teaches wherein the security processor resides on a network interface card (NIC) (outbound packets are loaded into the memory of NIC for processing) (Yang, col. 5, lines 60-66).

As to claim 40, Yang teaches:

a. Receiving a TCP/IP packet in a data flow and storing context information associated with the TCP/IP packet (the processor of Yang is used in the TCP environment and receives packets and saves data about those packets) (Yang, col. 2, lines 8-26 and col. 5, line 58-col. 6, line 9).

b. Identifying flow identification information for the data flow including a flow identifier (packet has an SA_ID (flow identifier) and data indicating the type of security processing required) (Yang, col. 5, line 58-col. 6, line 9).

c. Generating the internal packet including a security identifier header having the flow identifier, a security processor address data, and at least a portion of the TCP/IP packet (IPSEC Tx Data State Machine generates and assembles

outbound packet after processing with header data. Packet has an SA_ID (flow identifier) , data indicating the type of security processing required and the SA_ID is an index (address) used to lookup SA fields for IP processing) (Yang, col. 7, lines 28-49 and col. 5, line 58-col. 6, line 48).

d. Transmitting the internal packet to the security processor over the PCI bus for cryptographic processing (required processing is executed on the outbound packet to include cryptographic operations) (Yang, col. 6, line 66-col. 7, line 8).

As to claim 56, Yang teaches the at least one Ethernet controller securely communicates with the at least one security processor to configure the at least one security processor or retrieve status information from the at least one security processor (various processors within the architecture of Yang communicate with each other in order to properly process outbound packets) (Yang, col. 5, line 58-col. 6, line 9).

As to claims 60 and 61, Yang teaches prior to receiving the internal outbound packet in a flow, receiving security association information for the flow, the security association information handle and security association data (security association data is stored in the memory of the NIC and is present before the packet is processed by the hardware) (Yang, col. 5, lines 58-col. 6 line 9).

As to claim 62, Yang teaches the security processor is part of a computer system (Yang, col. 10, lines 29-53).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

13. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

14. Claims 8-10, 12, 15, 21-23 and 65-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,003,118 to Yang et al. (hereinafter Yang) in view of US Patent No. 7,162,630 to Sperry et al. (hereinafter Sperry).

As to claim 8, Yang teaches:

a. Receiving, by a security processor, an internal outbound packet from an Ethernet controller (the apparatus of Yang is used in an Ethernet environment) (Yang, col. 2, line 60-col. 3, line 4), wherein the internal outbound packet includes a flow identifier for the internal outbound packet and a security processor address data (packet has an SA_ID (flow identifier) , data indicating the type of security processing required and the SA_ID is an index (address) used to lookup SA fields for IP processing) (Yang, col. 5, line 58-col. 6, line 48).

b. Processing at least a portion of the received internal outbound packet if the security processor address data matches address information associated with the security processor (SA_ID is used as an index lookup to apply IP processing to the packet. It is inherent, if not obvious, that the indices have to match in order for the IP processing to be executed on the packet.) (Yang, col. 6, lines 1-48), wherein the processing includes:

i. Using the flow identifier as a direct address handle to retrieve a security association for the received internal outbound packet (SA_ID is the security association identification associated with the packet and is

used as an index to obtain the appropriate keys for the packet) (Yang, col. 6, lines 52-65).

ii. Performing a cryptographic operation on a portion of the received internal outbound packet using at least a portion of the retrieved security association (required processing is executed on the outbound packet to include cryptographic operations) (Yang, col. 6, line 66-col. 7, line 8).

iii. Assembling an outbound network packet including a header and the cryptographically processed portion of the received internal outbound packet (IPSEC Tx Data State Machine assembles outbound packet after processing) (Yang, col. 7, lines 28-49).

iv. Transmitting from the security processor, the outbound network packet (IPSEC Tx Data State Machine transmits outbound packet after processing) (Yang, col. 7, lines 28-49 and fig. 4).

Yang does not expressly mention the use of a Media Access Controller. However, in an analogous art, Sperry teaches at least one Media Access Controller (MAC) (Sperry, col. 8, lines 25-32).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the IPSec processing of Yang with the Media Access Controller engine of Sperry in order to increase the speed and flexibility for communication security as suggested by Sperry (Sperry, col. 3, lines 40-50).

As to claim 9, Yang as modified teaches the at least one processor comprises at least one IPSec processor (the IPSec processing tasks are handled by the NPPs (Network Protocol Processors) (Sperry, col. 9, lines 41-45).

As to claim 10, Yang as modified teaches the IPSec processor is configured to add IPSec protocol elements to or to remove IPSec protocol elements from the internal outbound packet or the outbound network packet (adding IP elements (e.g., encryption, authentication) (Yang, col. 6, line 49-col. 7, line 8).

As to claim 12, Yang as modified teaches at least one data memory for storing security association information for use by the at least one processor, wherein the security information includes a handle and security association data (accessing security association data which includes identifying data that is used to properly handle data packets) (Sperry, col. 12, line 65-col. 13, line 15).

As to claim 15, Yang as modified teaches wherein the security processor resides on a network interface card (NIC) (outbound packets are loaded into the memory of NIC for processing) (Yang, col. 5, lines 60-66).

As to claim 21, Yang teaches:

a. Receiving, by a security processor, an internal outbound packet from an Ethernet controller (the apparatus of Yang is used in an Ethernet

environment) (Yang, col. 2, line 60-col. 3, line 4), wherein the internal outbound packet includes a flow identifier for the internal outbound packet and a security processor address data (packet has an SA_ID (flow identifier) , data indicating the type of security processing required and the SA_ID is an index (address) used to lookup SA fields for IP processing) (Yang, col. 5, line 58-col. 6, line 48).

b. Processing at least a portion of the received internal outbound packet if the security processor address data matches address information associated with the security processor (SA_ID is used as an index lookup to apply IP processing to the packet. It is inherent, if not obvious, that the indices have to match in order for the IP processing to be executed on the packet.) (Yang, col. 6, lines 1-48), wherein the processing includes:

i. Using the flow identifier as a direct address handle to retrieve a security association for the received internal outbound packet (SA_ID is the security association identification associated with the packet and is used as an index to obtain the appropriate keys for the packet) (Yang, col. 6, lines 52-65).

ii. Performing a cryptographic operation on a portion of the received internal outbound packet using at least a portion of the retrieved security association (required processing is executed on the outbound packet to include cryptographic operations) (Yang, col. 6, line 66-col. 7, line 8).

iii. Assembling an outbound network packet including a header and the cryptographically processed portion of the received internal outbound

packet (IPSEC Tx Data State Machine assembles outbound packet after processing) (Yang, col. 7, lines 28-49).

iv. Transmitting from the security processor, the outbound network packet (IPSEC Tx Data State Machine transmits outbound packet after processing) (Yang, col. 7, lines 28-49 and fig. 4).

Yang does not expressly mention the use of a Media Access Controller. However, in an analogous art, Sperry teaches at least one Media Access Controller (MAC) (Sperry, col. 8, lines 25-32).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the IPSec processing of Yang with the Media Access Controller engine of Sperry in order to increase the speed and flexibility for communication security as suggested by Sperry (Sperry, col. 3, lines 40-50).

Yang as modified further teaches at least one switch for distributing or collecting packets between the at least one media access controller and the at least one security processor (the use of switches in the target environment) (Sperry, col. 7, lines 5-19).

As to claim 22, Yang as modified teaches at least one media access controller comprises at least one Gigabit MAC (Sperry, col. 8, lines 25-30).

As to claim 23, Yang as modified teaches the at least one security processor is further configured to allocate memory space associated with the security association

used by the at least one security processor (security association data is saved to NIC memory) (Yang, col. 5, line 58-col. 6, line 9).

As to claims 65 and 66, Yang as modified teaches prior to receiving the internal outbound packet in a flow, receiving security association information for the flow, the security association information handle and security association data (security association data is stored in the memory of the NIC and is present before the packet is processed by the hardware) (Yang, col. 5, lines 58-col. 6 line 9).

As to claim 67, Yang as modified teaches the security processor is part of a computer system (Yang, col. 10, lines 29-53).

As to claim 68, Yang as modified teaches the security processor is in-line with a data path of a packet network (Sperry, col. 6, lines 35-48).

15. Claims 16-18, 20 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,003,118 to Yang et al. (hereinafter Yang) in view of US Patent No. 6,157,955 to Narad et al. (hereinafter Narad).

As to claim 16, Yang teaches:

a. Receiving, by a security processor, an internal outbound packet from an Ethernet controller (the apparatus of Yang is used in an Ethernet environment)

(Yang, col. 2, line 60-col. 3, line 4), wherein the internal outbound packet includes a flow identifier for the internal outbound packet and a security processor address data (packet has an SA_ID (flow identifier) , data indicating the type of security processing required and the SA_ID is an index (address) used to lookup SA fields for IP processing) (Yang, col. 5, line 58-col. 6, line 48).

b. Processing at least a portion of the received internal outbound packet if the security processor address data matches address information associated with the security processor (SA_ID is used as an index lookup to apply IP processing to the packet. It is inherent, if not obvious, that the indices have to match in order for the IP processing to be executed on the packet.) (Yang, col. 6, lines 1-48), wherein the processing includes:

i. Using the flow identifier as a direct address handle to retrieve a security association for the received packet (SA_ID is the security association identification associated with the received internal outbound packet and is used as an index to obtain the appropriate keys for the packet) (Yang, col. 6, lines 52-65).

ii. Performing a cryptographic operation on a portion of the received internal outbound packet using at least a portion of the retrieved security association (required processing is executed on the outbound packet to include cryptographic operations) (Yang, col. 6, line 66-col. 7, line 8).

iii. Assembling an outbound network packet including a header and the cryptographically processed portion of the received packet (IPSEC Tx

Data State Machine assembles outbound packet after processing) (Yang, col. 7, lines 28-49).

iv. Transmitting from the security processor, the outbound network packet (IPSEC Tx Data State Machine transmits outbound packet after processing) (Yang, col. 7, lines 28-49 and fig. 4).

Yang does not expressly mention the use of a Media Access Controller. However, in an analogous art, Narad teaches a plurality of Media Access Controllers (MAC) (Policy Engine (PE) with two MACs) (Narad, col. 7, lines 63-67).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the IPSec processing of Yang with the multiple Media Access Controllers of Narad in order to accelerate the processing of packets as suggested by Narad (Narad, Abstract).

As to claim 17, Yang as modified teaches at least one processor comprises at least on IPSec processor (accelerator of Yang is used to process packets in an IPSec environment) (Yang, Title and Abstract).

As to claim 18, Yang as modified teaches the IPSec processor is configured to add IPSec protocol elements to or to remove IPSec protocol elements from the internal outbound packet or the outbound network packet (adding IP elements (e.g., encryption, authentication) (Yang, col. 6, line 49-col. 7, line 8).

As to claim 20, Yang as modified teaches at least one data memory for storing security association information for use by the at least one processor (Network Interface Card memory with security association data) (Yang, col. 5, lines 59-67).

16. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,003,118 to Yang et al. (hereinafter Yang) in view of US Patent No. 7,162,630 to Sperry et al. (hereinafter Sperry) as applied to claim 21 above, and further in view of US Patent No. 7,062,566 to Amara et al. (hereinafter Amara).

As to claim 24, Yang as modified does not expressly mention the use of VLAN tags. However, in an analogous art, Amara teaches the at least one switch associates VLAN tags with the at least one media access controller (VLAN tags are used as packet identifiers) (Amara, column 4, lines 12-36).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the IPSec scheme of Yang as modified with the VLAN tags of Amara in order to obtain the correct IPSec policies and apply them to the packet as suggested by Amara (Amara, column 4, lines 30-36).

17. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,003,118 to Yang et al. (hereinafter Yang) in view of US Patent No. 7,162,630 to Sperry et al. (hereinafter Sperry) in further view of US Patent No. 6,959,007 to Vogel et al. (hereinafter Vogel).

As to claim 27, Yang teaches:

a. Receiving, by a security processor, an internal outbound packet from an Ethernet controller (the apparatus of Yang is used in an Ethernet environment) (Yang, col. 2, line 60-col. 3, line 4), wherein the internal outbound packet includes a flow identifier for the packet and a security processor address data (packet has an SA_ID (flow identifier) , data indicating the type of security processing required and the SA_ID is an index (address) used to lookup SA fields for IP processing) (Yang, col. 5, line 58-col. 6, line 48).

b. Processing at least a portion of the received internal outbound packet if the security processor address data matches address information associated with the security processor (SA_ID is used as an index lookup to apply IP processing to the packet. It is inherent, if not obvious, that the indices have to match in order for the IP processing to be executed on the packet.) (Yang, col. 6, lines 1-48), wherein the processing includes:

i. Using the flow identifier as a direct address handle to retrieve a security association for the received internal outbound packet (SA_ID is the security association identification associated with the packet and is used as an index to obtain the appropriate keys for the packet) (Yang, col. 6, lines 52-65).

ii. Performing a cryptographic operation on a portion of the received internal outbound packet using at least a portion of the retrieved security

association (required processing is executed on the outbound packet to include cryptographic operations) (Yang, col. 6, line 66-col. 7, line 8).

iii. Assembling an outbound network packet including a header and the cryptographically processed portion of the received internal outbound packet (IPSEC Tx Data State Machine assembles outbound packet after processing) (Yang, col. 7, lines 28-49).

iv. Transmitting from the security processor, the outbound network packet (IPSEC Tx Data State Machine transmits outbound packet after processing) (Yang, col. 7, lines 28-49 and fig. 4).

Yang does not expressly mention the use of a Media Access Controller. However, in an analogous art, Sperry teaches at least one Media Access Controller (MAC) (Sperry, col. 8, lines 25-32).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the IPSec processing of Yang with the Media Access Controller engine of Sperry in order to increase the speed and flexibility for communication security as suggested by Sperry (Sperry, col. 3, lines 40-50).

Yang as modified further teaches:

c. At least one switch for routing packets between the at least one media access controller and the at least one security processor (the use of switches in the target environment) (Sperry, column 7, lines 5-19).

Yang as modified does suggest differing circuit layouts (Sperry, column 6, lines 35-48), but does not expressly use the terms backplane and blade in defining the architecture of the security processor. However, in an analogous art, Vogel teaches:

d. At least one backplane (Vogel, column 5, lines 17-33).

e. At least one processing blade connected to the at least one backplane (Vogel, column 5, lines 17-33).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the IPSec scheme of Yang as modified with the backplane and blade configuration of Vogel in order to achieve an architecture that is cheaper, requires a lower chip count, requires less power and provide adequate bandwidth as suggested by Vogel (Vogel, column 1, lines 48-52).

18. Claim 51 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,003,118 to Yang et al. (hereinafter Yang) as applied to claim 33 above, and further in view of US Patent No. 6,157,955 to Narad et al. (hereinafter Narad).

As to claim 51, Yang does not expressly mention the modification of checksums. However, in an analogous art, Narad teaches at least one security processor is further configured to modify at least one checksum in the security identifier header (updating checksum of the packet) (Narad, column 115, lines 7-22).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the IPSec scheme of Yang with the checksum

modification of Narad in order to ensure that network traffic performs properly as suggested by Narad (Narad, column 115, lines 7-22).

19. Claims 52 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,003,118 to Yang et al. (hereinafter Yang) as applied to claim 33 above, and further in view of US Patent No. 6,947,430 to Bilic et al. (hereinafter Bilic).

As to claims 52 and 53, Yang does not expressly mention adjusting the packet size. However, in an analogous art Bilic teaches modifying at least one maximum transmitted unit size in accordance with modifications the at least one security processor makes to at least a portion of the outbound network packets (there is a maximum packet size and the size of the payload is in direct proportion to the size of the at least one header) (Bilic, column 8, lines 10-37).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the IPSec scheme of Yang with the dynamic packet sizing of Bilic in order to achieve high-speed packet header processing as suggested by Bilic (Bilic, column 1, lines 12-15).

20. Claims 58 and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,003,118 to Yang et al. (hereinafter Yang) as applied to claim 1 above, and further in view of US Patent No. 6,157,955 to Narad et al. (hereinafter Narad).

As to claims 58 and 59, Yang does not expressly mention the option of a low power or sleep mode. However, in an analogous art, Narad teaches entering and leaving a low-power configuration mode upon receipt of appropriate signals and disabling and enabling data paths as appropriate (putting system into sleep mode and waking from said sleep mode) (Narad, col. 38, lines 58-67).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the IPSec scheme of Yang with the sleep mode of Narad in order to conserve power as suggested by Narad (Narad, col. 38, lines 58-67).

21. Claims 63 and 64 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,003,118 to Yang et al. (hereinafter Yang) in view of US Patent No. 7,162,630 to Sperry et al. (hereinafter Sperry) as applied to claim 8 above, and further in view of US Patent No. 6,157,955 to Narad et al. (hereinafter Narad)..

As to claims 63 and 64, Yang as modified does not expressly mention the option of a low power or sleep mode. However, in an analogous art, Narad teaches entering and leaving a low-power configuration mode upon receipt of appropriate signals and disabling and enabling data paths as appropriate (putting system into sleep mode and waking from said sleep mode) (Narad, col. 38, lines 58-67).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the IPSec scheme of Yang as modified with the sleep mode of Narad in order to conserve power as suggested by Narad (Narad, col. 38, lines 58-67).

Conclusion

22. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to WILLIAM S. POWERS whose telephone number is (571)272-8573. The examiner can normally be reached on m-f 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/W. S. P./
Examiner, Art Unit 2434

William S. Powers
Examiner
Art Unit 2434

10/10/2008

/ELLEN TRAN/
Primary Examiner, Art Unit 2434